REMARKS

1. Applicant thanks the Examiner for her kind assistance provided during a telephone interview on April 7, 2009. During said interview, Applicant pointed out to the Examiner that her reliance on the combination of Goertzel/Hibbard was misplaced because the combination, as have previously cited references, describes IP-based rate limiting and that the Claims of the subject Application are presented as a remedy to the deficiencies of IP-based rate limiting. The Examiner suggested that amending the Claims to describe more clearly that the client identifier described in the Claims is not an IP address could move the Application closer to allowance.

2. **35 U.S.C. § 112**

Claims 1 and 38 are rejected under 35 U.S.C. § 112, 2nd ¶ for failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention. More particularly, it is alleged that the Claims are incomplete because they omit essential steps.

The Office posits that, between the transmitting step and the step where the requests are processed, there should be a step that determines whether the request received is trusted or untrusted. Applicant respectfully disagrees.

Applicant respectfully points out that the allegedly missing step is implicitly described in the second and final clause of Claims 1 and 38:

"establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service. . ." and

"wherein untrusted logins comprise successful and unsuccessful logins from entities determined to lack a trust token."

Therefore, from the description of a trusted entity in the second clause and the description of an untrusted login in the final clause, the ordinarily-skilled practitioner would readily deduce that a determination of whether or not a request is trusted or untrusted is made by establishing that the entity requesting service is trusted, as evidenced by the submission of a trust token with the request.

Nonetheless, in the interest of advancing prosecution of the Application, Applicant amends Claims 1 and 38 by inserting the following step:

"determining whether each request is a trusted or an untrusted login. . . ."

Support for the amendment is implicit in the Claims in their previous condition. The new step merely explicitly states what was already implicitly described.

3. **35 U.S.C. § 103**

Claims 1 and 38 are rejected as being unpatentable over U.S. patent no. 6,308,273 ("Goertzel") and further in view of U.S. patent no. 7,454,794 ("Hibberd"). Applicant respectfully disagrees.

Applicant first notes that Goertzel is directed to a method and system of security location discrimination. Goertzel's abstract describes, "Based on information including the location and the user's credentials, an access token is set up that may restrict the user's normal access. . . "(emphasis added). Thus, Goertzel is directed to a different problem from the subject matter of the present Application. As described in the foregoing passage from the abstract, Goertzel concerns itself with the problem of associating a particular set of user credentials with a particular location. As Applicant has endlessly explained, the Claims of the subject Application are directed to a fine-grained method of applying rate-limiting to untrusted logins. In so doing a trust token is issued that associates a particular user ID with a particular machine or computer. Furthermore, this is done without the use of conventional IP-based rate-limiting.

Applicant has thoroughly discussed the disadvantages of conventional IP-based rate limiting strategies in the Application, at least at ¶¶ 4-21 and 49-54 of U.S. patent application pub. no. 2005/0108551.

As Applicant points out in the cited paragraphs, conventional IP-based rate limiting is an exceptionally coarse tool for differentiating friendly traffic from unfriendly traffic. Because IP-based rate limiting filters sets of hosts, it must deny service to a great deal of friendly traffic in order to protect a service from malicious traffic. Additionally, such measures are usually effective for only a

short while before a cracker is able to circumvent them. Also, because of the transitory nature of many IP addresses, IP address-based countermeasures for a particular IP address are only good for as long as the IP/user binding persists.

Applicant's remedy for the deficiencies of conventional IP-based rate limiting is a method for ap plication of trus t-based, fine grained rate limiting, wherein trust is extended to unique client-user pairs. Trust is established by issuing a trust token to a unique client-user ID pair.

The Office relies on Goertzel, col. 6, lines 30-35 and col. 7, lines 5-9 as teaching or suggesting: "said user id-client pair comprising an individual user-machine combination. . . ." Applicant respectfully disagrees. The col. 6 teaching describes the assignment of IP addresses to particular users according to the location from which a user is connecting. Accordingly, the user is associated to an IP address, that, itself is associated to a particular geographic location. The col. 7 teaching describes association of an IP address with a user according to a telephone number that the user is connecting from. Thus, again, the user is associated to an IP address that itself is associated to a particular telephone number. Thus, Goertzel uses IP addresses that are themselves associated to a particular location to associate a user to a location.

Claim 1 has nothing to do with associating a user to an IP address or to a location.

Goertzel's location-based association of IP addresses suffers all of the deficiencies that Applicant describes in the subject application. For example, the IP/user binding is temporary. Therefore, any IP-based countermeasures are only good for the duration of the IP/user binding. Additionally, again because the IP address associated to the user, as described in the cited passages of Goertzel, is primarily associated to the user's location, there is no establishment of a trusted user/machine entity.

The remaining teachings cited by the Office describe different permutations of IP-based rate limiting. Hibberd describes assignment of an ID to a client by a server, during a registration process. Thus, Hibberd adds nothing to Goertzel.

Unlike the conventional strategies described in the combination, the subject Application describes countermeasures applied to single user-machine pairs. There is no teaching or suggestion in Goertzel, or in the combination, that countermeasures be applied to unique client-user pairs.

Accordingly, because the combination fails to teach or suggest all elements of Claim 1, the present rejection is deemed improper. Claim 1 is therefore allowable over the combination. The foregoing Applies equally to Claim 38. Claim 38 is therefore allowable for the same reasons that Claim 1 is allowable.

In view of their dependence from allowable parent Claims, the dependent Claims are deemed allowable without any separate consideration of their merits.

Even though Applicant's position is that that the rejection of Claims 1 and 38 is improper, in recognition of the Office policy of compact prosecution, Applicant amends Claims 1 and 38 to describe that the client identifier comprises at least one item of client-originated data unique to the client machine. Support for the amendment is found at ¶¶ 0092-0093 of U.S. patent application pub. no. 2005/0108551. No new matter is added by way of the amendment.

Goertzel describes the association of IP addresses to individual users (Col. 6, lines 30-35); and the IP address is itself associated with a location. Accordingly, the association between the user and the IP address only lasts, at most, for as long as the user is at the location. Thus, there never exists an association of the IP address to a client machine. Even if the IP address were associated to the user's client machine, the association is fleeting, lasting no longer than the time the user is at the location. After that, the IP address is available for reassignment; it is therefore not unique to the client. Hibberd adds nothing to Goertzel. Hibberd describes assignment of an ID to a client by a server during a registration process. Thus, the assignment of the ID takes must occur before the user ever logs on to the server successfully. Additionally, because the ID is generated and assigned by the server, it is not client-originated.

Unlike Goertzel/Hibberd, the present approach uses for a client ID a data item that is unique to the client and that originates with the client, unlike an IP

address that is assigned by a server and that can be quickly associated to another user. Because the data item is originated by the client, it is truly unique to the client, not just for a brief period, as in an IP address that is temporarily associated to the user of a client.

Therefore, even if the present rejection were not improper, it would be overcome by the present amendment. Claims 1 and 38 are therefore deemed allowable over the combination. In view of their dependence from allowable parent Claims, the dependent Claims are deemed allowable without any separate consideration of their merits.

Claims 10, 29, 37, 47, 66 and 74 are rejected as being unpatentable over Goertzel/Hibberd in view of U.S. patent application pub. no. 2003/0028495 ("Pallante"). In view of the foregoing, the present rejection is deemed improper/overcome.

Claims 34 and 71 are rejected as being unpatentable over Goertzel/Hibberd in view of U.S. patent application pub. no. 2002/0073339 ("Card"). In view of the foregoing, the present rejection is deemed improper/overcome.

Claim 69 is rejected as being unpatentable over Goertzel/Hibberd in view of U.S. patent application pub. no. 2002/0032793 ("Malan"). In view of the foregoing, the present rejection is deemed improper/overcome.

4. For the record, Applicant respectfully traverses any and all factual assertions in the file that are not supported by documentary evidence. Such include assertions based on findings of inherency, assertions based on official notice, and any other assertions of what is well known or commonly known in the prior art.

5. No new matter is added by way of the above amendments. The foregoing amendments are made only for expediency, in the interest of advancing prosecution of the Application. They do not signify agreement with the Examiner's position. Nor do they reflect intent to forsake claim scope. Applicant

expressly reserves the right to pursue protection of a scope it reasonably believes it is entitled to in one or more continuing submissions to the USPTO.

CONCLUSION

In view of the foregoing, the Application is deemed to be in allowable condition. Therefore, Applicant respectfully requests reconsideration and prompt allowance of the claims. Should the Examiner have any questions regarding the Application, he is urged to contact Applicant's Attorney at 650-474-8400.

Respectfully submitted,

Elizabeth Ruzich
Reg. No. 54,416

Customer No. 22862